



***2009 High Technology Crime In California:
Annual Report to the Governor & Legislature***

PROLOGUE

It is the intention of this report to provide that information necessary to inform, disseminate, educate, and define cybercrime, as well as the approach and effect of the five state-funded high technology and identity theft task forces to that challenge. This annual report to the Governor will encompass the following:

- Cybercrime defined.
- Executive Summary by San Diego County Deputy District Attorney (DDA) and Project Director Brian McHugh of the San Diego High Technology and Identity Theft Task Force (CATCH).
- Comments from William E. Eyres, Chairman, High Technology Crime Advisory Committee CalEMA
- Task force statistics.
- Task Force History.
- Task Force Profiles to include individual cases highlighted during the fiscal period of 2008-2009 of each task force. This is intended to provide the task forces an opportunity to showcase their hard work.
- Observations from the top administrator of the agencies that represent the task forces. This is an opportunity to hear the voices behind the task force.
- Remarks from Santa Clara County DDA and California District Attorney's Association (CDAA) representative Bud Frank (member of the High Technology Advisory Committee, HTCAC).

CYBERCRIME DEFINED

Cybercrimes are generally defined as any type of illegal activity that makes use of the Internet, a private or public network, or an in-house computer system. The directed groups of attacks are the following three categories: Personal, Property, or Government. The components of cybercrime are listed in the following:

- | | |
|----------------------------------|--|
| • Malware and malicious code | • Cyber Terrorism |
| • Denial-Of-Service Attacks | • Extortion |
| • Computer viruses | • Counterfeit and Piracy |
| • Cyber stalking | • Email extortion |
| • Theft of Intellectual Property | • Reshipping* |
| • Identity Theft | • Phishing ¹ , pharming ² , spearing ³ , and whaling ⁴ |
| • Network intrusions (hacking) | • Auction Fraud |

¹ **Phishing** is the process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public to enter details at a fake website whose look and feel are almost identical to the legitimate one.

² **Pharming** is a hacker's attack aiming to redirect a website's traffic to another, bogus website.

³ **Spearing** is a narrowly focused variant of phishing. Rather than bottom trawling the Internet by sending massive numbers of generic messages, spear-phishers gather detailed personal information readily available via Google and Social Networking

⁴ **Whaling** is targeted phishing attacks on senior executives.

EXECUTIVE SUMMARY

California is the nation's leader in High Tech industries and was recently described as, "an unparalleled engine of innovation, the [M]ecca of high tech, biotech and now clean tech."⁵ In the Milken Institute's report on North America's High-Tech Economy, five California metropolitan regions are ranked among the top ten high-tech centers in North America.⁶ California ranked first in the nation in the recent Cyberstates 2009 report, in the employment categories of: computer systems design and related services; communications services; Research and Design and testing labs; and engineering services.⁷ Californians are a very tech savvy population, with 80% of Californians using a computer at home, work, or school; 76% accessing the Internet; 37% using social network sites, an increase of 11 percent from 2008; and 58% shopping online.⁸

Unfortunately, California also continues to be a leader in High Tech crime statistics. According to the most recent Internet Crime Complaint Center (IC3), Internet Crime Report, of the 275,284 internet crime complaints received in the 2008 calendar year, Californians comprised 15.8% of the identified internet crime perpetrators and 14.6% of the victims.⁹ The Federal Trade Commission reported 51,140 Identity Theft Complaints from Californians in 2008 and ranked 6 California metropolitan areas in the top ten largest metropolitan areas for Identity Theft related complaints.¹⁰

High Tech crime and Identity Theft statistics continue to rise in a difficult economy. Cyber-criminals are becoming increasingly organized and a shadow economy has developed where malicious software, lists of target emails, rented time on botnets, and blocks of comprised credit card numbers can be bought and sold.¹¹

The National White Collar Crime Center (NW3C) reported that IC3 received 327,251 complaints from July 2008 to June 2009, which is an increase of nearly 100,000 complaints from the previous fiscal year when IC3 received 232,495 complaints.¹² High Tech crime is on the rise across the nation, mirroring the increasing use and proliferation of technology. The Identity Theft Resource Center reports that in 2008, data breaches of personal identifying information increased by 47% with 656 reported breaches in 2008 as compared to 446 in 2007.¹³ Tiversa research revealed 13,185,252 breached files emanating from Peer to Peer file-sharing networks between March 2008 and March 2009 and an unprecedented 32% increase in Identity Theft related internet searches during the fall of 2008.¹⁴ According to a recent study by the Congressional Research Service, Identity Theft similarly is on the rise, with about 9.9 million victims in 2008, an increase of 22% over 2007.¹⁵

⁵ Time, Despite Its Woes, California's Dream Still Lives: <http://www.time.com/time/nation/article/0,8599,1931582-1,00.html>

⁶ Milken Institute: <http://www.milkeninstitute.org/publications/publications.taf?function=detail&ID=38801199&cat=resrep>

⁷ TechAmerica: <http://www.techamerica.org/cyberstates-2009-san-diego>

⁸ Public Policy Institute of California: http://www.ppic.org/content/pubs/survey/S_609MBS.pdf

⁹ Internet Crime Complaint Center, 2008 IC3 Annual Report: <http://www.ic3.gov/media/annualreports.aspx>

¹⁰ Federal Trade Commission, Consumer Sentinel Network Data Book for January-December 2008:

<http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>

¹¹ Sarah Arnott, "How Cyber Crime Went Professional," The Independent," August 13, 2008:

<http://www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html> and

Finjan Malicious Code Research Center, Web Security Trends Report Q4 2008: <http://www.finjan.com/Content.aspx?id=827> and

Trend Micro 2008 Annual Threat Roundup and 2009 Forecast:

http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

¹² National White Collar Crime Center, NW3C Annual Report 2008-2009 and NW3C Annual Report 2007-2008:

http://www.nw3c.org/research/site_files.cfm?mode=p

¹³ Identity Theft Resource Center:

http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml

¹⁴ Digital Communities, New Trend in Cyber Crime: Unprecedented Rise in Identity Theft Related Searches:

<http://www.govtech.com/dc/592233> and Tiversa:

http://www.tiversa.com/media/press/2009/2009_05_28_Tiversa_Identifies_Over_13Million.html

¹⁵ Congressional Research Service, Identity Theft: Trends and Issues: <http://www.fas.org/sgp/crs/misc/R40599>

California has taken an innovative approach to fighting High Tech crime and Identity Theft. Since the inception of the High Technology Theft Apprehension and Prosecution Program (HTTAP) in 1998, California has combated High Tech crime with a task force approach. The task force approach was adopted because High Tech criminal organizations are sophisticated and extend over multiple jurisdictions making it extremely difficult for smaller departments to maintain the expertise, equipment and ability to maintain centralized data bases.¹⁶ The multi-agency and multi-jurisdictional task forces are comprised of federal, state, and local investigators and prosecutors. Within the five HTTAP task forces working together to combat High Tech crime and Identity Theft across California, there are at least 30 local police departments, 15 sheriff's departments, 3 probation departments, 15 district attorney's offices, 5 state investigative agencies, the Attorney General's Office, 5 federal investigative agencies and the United States Attorney's Office. The California District Attorneys Association and the California Department of Justice, Office of the Attorney General, support the task forces by providing legal research, training, and a statewide intelligence database.

While the High Tech crime and Identity Theft trends have been expanding over the years, the funding of the HTTAP task forces has diminished. In 2008-2009 the combined task forces funding decreased by roughly 4 million dollars from that of the 2007-2008 and 2006-2007 fiscal years, affecting the ability of the task forces to effectively investigate and prosecute High Tech crime and Identity Theft. The combined data of the HTTAP task forces for the last three years reveals that despite the aggressive growth of High Tech crime and Identity Theft in the last fiscal year, the number of investigations, cases filed, and convictions have declined across the state, mirroring the decrease in funding. However, the task force data also shows a correlation to the reports of an increase in the amount of crime, because the number of victims and the amount of loss have dramatically risen compared to the previous years.

The task force investigators require a tremendous amount of training to stay abreast of the developing technology and trends, so that investigators can understand how criminals are using constantly changing technology to victimize the population and how evidence of that crime can be detected. The investment into training investigators matures into real rewards as those investigators fully develop with significant experience investigating crimes of this sort. It takes a substantial amount of training and experience for an investigator to develop the expertise to be able to conduct the investigations, forensic analysis, and be able to convey that information to a jury in an easily understandable manner. The disruption in funding in the last fiscal year caused many personnel changes as local agencies had to re-evaluate whether they could bear the increased costs as State funding dwindled. These changes had dramatic effects on the task forces' composition and investigative capabilities that are apparent from the decline in investigations, cases filed and convictions over the last fiscal year.

Despite the challenges that the task forces faced in 2008-2009, due to the budget dynamics, they continue to bring a significant return on the investment of State funds. The combined total of the State's contribution and the task forces' 25% match represents a \$12,398,228 investment that yielded the investigation of crimes effecting 1,553,533 victims for an aggregated loss of \$313,929,108. California is a major stakeholder in High Technology, as an industry important to our economy, as a critical infrastructure to businesses, and as an ever increasing importance to our private lives. In order to keep pace with the increasing trends in High Tech crime and Identity Theft, the High Technology Theft Apprehension and Prosecution Program needs a stable commitment of resources sufficient to maintain adequate staffing levels of trained, experienced investigators. With such a commitment, the HTTAP task forces will have the tools necessary to effectively interdict and combat High Tech crime and Identity Theft in California.

¹⁶ Senate Committee on Public Safety 4/15/98: http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_1734&sess=9798&house=B&author=johnston

LETTER FROM THE HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE CHAIRMAN

Dear Governor Schwarzenegger, Senate President pro Tem Darrell Steinberg, and Speaker of the Assembly Karen Bass:

In the ten years that the High Technology Task Force has been in existence the growth of technology has been dramatic. During those early years Computer forensic examinations were the single most important need facing law enforcement and computer storage was measured in megabytes. Today's cell phones have gigabytes of memory more than those computers of the 1990's and memory is now measured in Terabytes (1000 billion bytes). California's high tech industry including software development, entertainment (movies, recording and gaming) communications, computing, banking services, online auctions leads the world. These industries are the lifeblood of our state and their contributions to our state cannot be overstated. Likewise our citizens are users of these technologies and are being victimized by the various crimes being investigated by the Task Force.

These dramatic changes have been challenging for the men and women who comprise the California High Technology Task Force. The task force was mandated by Section 13848 of the Penal Code. This program provides objectives, direction and funding of five high tech and identity theft task forces supported by the California Department of Justice and the California District Attorneys Association. Each unit consists of local, state and federal law enforcement and prosecutorial personnel. All of these members receive the best possible training on an ongoing process to keep current with the changing technology and investigative techniques. The perpetrators of these high tech crimes and identity thefts have also gotten better and have devised new ways to commit old crimes and created new crimes based on technology.

As you can imagine this constant struggle to stay with the changing technology and one step ahead of the criminal is difficult in the best of times. During this reporting period the state budget crisis and the lack of clear funding direction hampered their work. The need for a stable funding process that realistically provides long term growth for the task force efforts is the highest priority. You will see as you read the report that the work of the Task Force is a good use of state and local funds. The investment of a little over \$12 million, counting local 25% match, lead to the investigation of crimes effecting 1.5 million victims with an aggregated loss of \$314 million!

This report details the efforts during the 2008-2009 funding cycle. I urge you to read the report and give careful consideration to the information contained in it and the recommendations being put forward.

Respectfully Submitted

William E. Eyres

Chairman, High Technology Crime Advisory Committee
CalEMA

GRANT FUNDING & STATISTICAL CRIME DATA

Task Force	Cal-EMA Grant Funding \$		Matching Funds \$ from lead agency	Combined Total \$
	ID	HT		
CDA				226,463.00
DOJ Database				54,716.00
DOJ DAG	399,440.00		99,860.00	499,300.00
REACT	407,022.00	1,420,691.00	456,929.00	2,284,642.00
CATCH	407,022.00	1,420,691.00	456,929.00	2,284,642.00
NC3	407,022.00	1,420,691.00	456,929.00	2,284,642.00
SCHTTF	407,022.00	1,420,691.00	456,929.00	2,284,642.00
SVHTCTF	407,022.00	1,420,691.00	456,929.00	2,284,642.00
Total:				\$12,203,689.00

High Tech Investigations								
Task Force	Cases Investigated	# of Victims	\$ loss	Arrests	Charges Filed	Convictions	Forensic Exams	Presentations
REACT	102	188	7,148,899.00	28	14	12	82	5
CATCH	183	32	339,058.00	12	11	7	103	13
NC3	156	152	13,927,059.00	53	39	13	186	4
SVHTCTF	316	317	4,211,365.00	0	7	15	350	24
SCHTTF	29	8	1,200,000.00	64	0	0	225	4
TOTALS	786	697	26,826,381.00	157	71	47	946	59

Identity Theft Investigations								
Task Force	Cases Investigated	# of Victims	\$ loss	Arrests	Charges Filed	Convictions	Forensic Exams	Presentations
REACT	94	498	1,221,544.00	50	26	13	79	12
CATCH	36	34	3,836,610.00	15	17	23	0	2
NC3	28	62	454,645.00	11	10	0	0	6
SVHTCTF	372	1,501,240	7,234,457.00	134	382	232	28	41
SCHTTF	0	51,002	14,331,471.00	287	120	54	0	14
DOJ DAG ID	2	0	260,024,000.00	5	22	63	0	18
TOTALS	532	1,552,836	287,102,727.00	502	577	385	107	93

TASK FORCE HISTORY

In 1998, the Task Force Bill was passed by the legislature and signed by, then, Governor Pete Wilson. At the stroke of a pen the grants were awarded to Southern California (SCHTTF), Sacramento (SVHTCTF), and the Silicon Valley/Bay Area (REACT) in 1999. A year later (2000) the North Bay Task Force (NC3TF) and the San Diego Task Force (CATCH) were added to the group bringing the total number of task forces to five that remain to this day. In 2001, the task forces received additional grants to combat Identity Theft. The following information identifies the five task forces and the jurisdictions they serve:

TASK FORCE PROFILES

RAPID ENFORCEMENT ALLIED COMPUTER TEAM (REACT)

Lead Agency: ***Santa Clara County District Attorney's Office***

REACT is represented by the following five counties:

- Alameda
- San Francisco
- San Mateo
- Santa Clara
- Santa Cruz

Through a common memorandum of understanding (MPO), **REACT** is comprised of participants from the following agencies:

- | | |
|---|--|
| • Santa Clara County District Attorney's Office (Investigators and DDA's) | • Department of Motor Vehicles |
| • Santa Clara County Sheriff's | • United States Secret Service |
| • San Mateo County Sheriff's (Investigators and DDA's) | • United States Postal Inspector |
| • San Jose Police Department | • San Francisco County District Attorney's Office |
| • Fremont Police Department | • Alameda County District Attorney's Office |
| • Mountain View Police | • State Attorney General's Office |
| • Pacifica Police Department | • Federal Bureau of Investigations (FBI) liaison |
| • Millbrae Police Department | • San Jose State Parole liaison |
| • Atherton Police Department | • US Immigration and Customs Enforcement (ICE) liaison |
| • California Highway Patrol | • Department of Motor Vehicles |

CASE PROFILES

Between July 2008 and January 2009, the REACT Task Force conducted a criminal investigation regarding a Visa International employee. The suspect worked for Visa as an Information Technology (IT) Technician. Over Approximately two (2) years, the suspect utilized the Cisco website to create false service requests for replacement parts, wherein he returned older, out-of-date, parts that he removed from Visa servers that were no longer in service. The suspect then sold the newer obtained parts on the grey market causing a loss of approximately \$2 million for Cisco and an undetermined loss to Visa.

The criminal investigation discovered that the suspect had a gambling habit, which he was supporting with his criminal gains. An arrest warrant was obtained for the suspect and he was subsequently arrested out of state and extradited back to California on charges related to theft by false pretense, embezzlement, and other related charges.

The suspect pleaded nolo-contendere to Grand Theft and enhancements. The suspect was sentenced to 1 year county jail; 5 years supervised probation, and restitution in the amount of \$1,538,000.00.

In December 2008, a REACT Task Force Agent received two fraud reports from the San Francisco District Attorney's Office. Two unrelated victims alleged falling victim to a Craigslist fraud perpetrated by a French national who was then residing in San Bruno, CA. The suspect offered to sell both victims discounted airline tickets. He met the victims, took their money, and failed to provide the tickets. Through the investigation, REACT discovered that the suspect had been investigated by numerous local police agencies around the country. In each instance, the case was closed without prosecution for either lack of jurisdiction or as a case "better pursued in civil courts". It was also determined that the suspect was on probation for check fraud.

Additional victims were located and a larger case was developed against the suspect as a prolific fraudster. Through further investigation, approximately 34 victims were located with a documented loss of approximately \$20,000. In subsequent interviews, the suspect admitted to committing his frauds. He is a serial scammer who would not have been brought to justice if not for REACT's ability to investigate cases across traditional jurisdictional boundaries and close working relationship with the District Attorney's Office.

Currently, the San Mateo County District Attorney's Office plans to file approximately 22 counts of theft by false pretense and 22 counts of grand theft against the suspect. To date, the complaint and arrest warrant are pending a final forensic search of the suspect's computer and phone for additional victims.

In 2008-2009, the REACT Task Force investigated two cases involving three suspects who conspired to steal credit card numbers via a technique known as "skimming" and use the stolen credit card numbers to purchase gift cards. The gift cards were later sold or used to purchase products from various retailers. The known loss associated with the conspiracy was over \$100,000.

The three suspects involved in the conspiracy were: a waiter at an Indian restaurant in Burlingame, CA (Suspect 1); his wife, a deli employee at a grocery store in South San Francisco (Suspect 2); and an unemployed male living in Pacifica, CA, who was the mastermind of the operation (Suspect 3). Suspect 3 recruited the waiter and provided him with a palm sized device called a "skimmer". The device could read the credit card numbers encoded to the magnetic strip on the back of credit cards and retain up to 5000 card numbers for later retrieval. The waiter would then return the skimmer to

Suspect 3 in exchange for a fee. Suspect 2 used her position as a clerk at a grocery store to covertly purchase gift cards with the stolen credit card numbers. Suspect 1 would then provide the gift cards to Suspect 3 who would sell them or use them to purchase product for later re-sale.

Hundreds of victims were identified and thousands of dollars were lost as a result of this year long conspiracy. Multiple search warrants were executed and all three suspects were arrested, later pleading out to three year sentences in prison.

COMMENTS

"The most serious concern about this unprecedented budgetary crisis facing REACT is that it may take away, or substantially reduce, our ability to protect a community that we have been so determined and committed to protect over the years."

Dolores Carr
District Attorney, Santa Clara County

"Because high-tech crimes are perpetrated across jurisdictions and geographical boundaries, the inability of local agencies to work together in a collaborative fashion will set all of our agencies behind. We at the San Jose Police Department are especially concerned that the loss of our region's ability to stay on top of high-tech crimes will provide criminals with an opportunity to grow their criminal enterprises and put law enforcement in a catch-up mode for years to come."

Rob Davis
Chief of Police, San Jose Police Department

"For over a decade investigators from local, state, and federal agencies have banded together as part of the REACT task force to maximize scarce resources and stay one step ahead of a new and rapidly evolving generation of criminal."

Thomas Ravenelle
Assistant Special Agent in Charge
FBI - San Jose Office

"We can rely on... REACT to assist us on major cases when we need specialized help. That kind of experience helps to create the future leaders of our department."

Scott S.G. Vermeer
Police Chief, City of Mountain View

"Those who commit fraud using the Internet can easily bilk citizens for hundreds of thousands of dollars from the comfort of their own home, or any location with Internet access without ever risking confrontation with their victims, other citizens or the police on the streets. With relatively few investigative resources and even less prosecutorial resources, the chances of actually being caught and brought to justice are slim. Therefore, suspects who engage in ID theft know that it is already 'Open Season' on our already depressed bank accounts, credit cards and credit scores."

Greg Munks
Sheriff, San Mateo County

"REACT is simply too valuable to lose. In today's economy the Fremont Police Department could not dedicate two investigators to handle High Tech crime and be nearly as effective as a task force concept. Numerous cases have been made by the REACT team and have actually helped in bringing

new High Tech industry to California and keeping those that we have due to the special relationships and partnerships that have been developed over the life of REACT with our High Tech partners. Of all the task force groups we participate with REACT is by far the most effective."

Craig Steckler
Chief of Police, Fremont Police Department

COMPUTER AND TECHNOLOGY CRIME HIGH-TECH RESPONSE TEAM (CATCH)

Lead Agency: ***San Diego County District Attorney's Office***

CATCH is represented by the following three counties:

- Imperial
- Riverside
- San Diego

Through a common memorandum of understanding, **CATCH** is comprised of participants from the following agencies:

- | | |
|---|---|
| • California Department of Justice | • Riverside County Sheriff's Department |
| • California State Parole | • San Diego County District Attorney's Office |
| • California Department of Motor Vehicles | • San Diego County Probation |
| • Carlsbad Police Department | • San Diego County Sheriff's Department |
| • Federal Bureau of Investigations (FBI) | • San Diego Police Department |
| • Imperial County District Attorney's Office | • United States Postal Inspector |
| • Riverside County District Attorney's Office | • Riverside County Sheriff's Department |

CASE PROFILES

While working at a Verizon phone store, the defendant copied the data in customer files and used multiple victims' credit card account numbers to buy \$6,800.00 worth of high-tech items online. The defendant then sold the stolen merchandise on Craig's List. An additional \$6,300.00 worth of fraudulent orders were caught by online retailers and cancelled before delivery. When the defendant was questioned he explained that he saw a television show about identity theft and thought he could easily commit similar crimes. The Defendant entered guilty pleas to six felony counts, was ordered to pay \$7,307.25 in victim restitution, and serve 150 days in local custody on a five year grant of formal probation.

The victim in this case was a Deputy Sheriff and distant relative of the Defendant. The Defendant, a Mexican National, acquired a copy of the victim's birth certificate, applied for a California Driver's License and Social Security Number. The Defendant lived in Mexico and worked in the United States, crossing the border on an almost daily basis for ten years before the Internal Revenue Service confronted the victim about \$7,000 dollars of taxes owing on unreported income. The taxes and income were entirely attributable to the Defendant. The Defendant entered guilty pleas to four felony counts and one misdemeanor count, and was ordered to serve 180 days in local custody on a three year grant of formal probation.

Suspect 1 was on formal probation for Identity Theft crimes when she and Suspect 2 passed two forged checks for a total of \$1,189.81 at a local market. Suspect 1 was later contacted at her residence where the stolen mail, checks and profiles containing personal identifying information of forty (40) different victims were located. Among these items were checks drawn on the victim's checking account. The victim previously reported that his bank was contacted by an unknown person, who without his consent, changed the mailing address on his account, then ordered a new ATM card and new checks, which were subsequently used without his authorization. The day that the checks were delivered to the fictional address, Suspect 1 cashed one of the victim's checks at a nearby Money Tree location. Suspect 1 was sentenced to two (2) years state prison and Suspect 2 was granted formal probation.

The Defendant was the maintenance man at the victim's apartment complex. The victim noticed unauthorized 1-(900) charges on her phone bill, realized that the volume on her computer had been turned down, and that a pornography site had been visited on her computer. The victim installed a surveillance system inside her apartment and captured video of the Defendant masturbating inside the victim's apartment, looking at the same pornography site that was accessed previously. The Defendant entered guilty pleas to three felony counts, two of them strikes and was ordered to serve 365 days of local custody on a three year formal grant of probation.

NORTHERN CALIFORNIA COMPUTER CRIMES TASK FORCE (NC3TF)

Lead Agency: ***Marin County District Attorney's Office***

NC3TF is represented by the following thirteen counties:

- | | |
|----------------|------------|
| ● Contra Costa | ● Shasta |
| ● Del Norte | ● Siskiyou |
| ● Humboldt | ● Solano |
| ● Lake | ● Sonoma |
| ● Napa | ● Tehama |
| ● Marin | ● Trinity |
| ● Mendocino | |

Through a common memorandum of understanding, **NC3TF** is comprised of participants from the following agencies:

- | | |
|--|---|
| ● California Department of Justice | ● Novato Police Department |
| ● California Department of Motor Vehicles | ● Redding Police Department |
| ● Concord Police Department | ● San Pablo Police Department |
| ● Contra Costa County District Attorney's Office | ● Shasta County District Attorney's Office |
| ● Del Norte County District Attorney's Office | ● Shasta County Sheriff's Department |
| ● Federal Bureau of Investigation (FBI) | ● Solano County District Attorney's Office |
| ● Humboldt County District Attorney's Office | ● Sonoma County District Attorney's Office |
| ● Lake County District Attorney's Office | ● Tehama County District Attorney's Office |
| ● Marin County District Attorney's Office | ● Trinity County District Attorney's Office |
| ● Marin County Sheriff's Department | ● United States Postal Service |
| ● Mendocino County District Attorney's Office | ● United States Secret Service |
| ● Napa County District Attorney's Office | ● Vacaville Police Department |
| ● Napa County Sheriff's Department | ● Vallejo Police Department |

CASE PROFILES

The NC3TF received a request from the Cotati Police Department to assist in the investigation of a Child Exploitation case. An image of a pre-pubescent female, engaged in a sexual act with an adult male, was found to have been transmitted by the suspect.

While serving a search warrant at the suspect's residence, investigators found that the child depicted in the original photograph was that of the suspect's 9-year-old daughter.

Multiple computers and digital cameras were seized from the suspect's residence and examined by the NC3TF. Further search warrants resulted in the discovery of corroborating physical evidence.

In addition to simply identifying these relevant items, the NC3TF Investigator found even more embedded data from some photos, which enabled the prosecutor to put time frames on many of the offenses. This was instrumental in identifying patterns of behavior and explaining particular days to the jury so they could clearly understand what was happening.

The victim testified and corroborated some of the behavior that was evidenced in the photos, but according to the prosecutor, the photos and emails were the key to the case. At least 35 counts of the 46 count complaint were based solely on the photos and emails - production and distribution of child pornography. The NC3TF Investigator worked with the prosecutor, who, up to this point, had minimal computer knowledge. The NC3TF Investigator educated the prosecutor about the technical aspects of the Investigator's work. In addition, he helped her formulate the appropriate questions to ask him during trial.

The jury returned a verdict of guilty to all 46 counts including several that carry a life term (oral copulation and sexual penetration of a child under the age of 10 years) and multiple counts of child pornography including distribution and posing the child.

According to the prosecutor, this case could not have been prosecuted without the assistance and expertise of the NC3TF.

A case was referred to the NC3TF by the Vallejo and San Rafael Police Departments. The NC3TF is working the case with assistance from the Vallejo Police Department and the United States Postal Inspection Service.

A series of AT&T cellular store burglaries have occurred throughout California, with over 20 of the burglaries occurring in NC3TF jurisdiction. Thefts linked to the same suspects have occurred or been attempted in Las Vegas, NV; Vancouver, WA; and Portland, OR. The loss to AT&T is approximately \$800,000.

Through the analysis of cell phone records and cell tower data, 4 suspected burglars have been identified. Through follow up on stolen phones that have since been activated, 3 "fences" have been identified on eBay and Craigslist. Multiple undercover buys have been made through eBay and Craigslist which have confirmed that these subjects are selling phones stolen in these burglaries. Call data obtained through PEN Registers have linked the fences to the burglars. Indictments are currently being prepared by the US Attorney's Office for the arrests of 5 suspects.

The NC3TF received a complaint from the Marin County based company, Autodesk. The complaint was about a person advertising the sale of AutoCAD 2010 on Craigslist.

The ad listed the product for sale for \$100.00. The MSRP for the product is \$3,995.00. The ad also had a link to the Autodesk web site for more information on the product.

The NC3TF contacted the suspect by e-mail and arranged to purchase a copy of the software. During the undercover buy, the suspect informed the NC3TF agent that the suspect had a relative who worked at Autodesk and this is how he is able to sell the software at this price. During this purchase the suspect showed the NC3TF agent additional software he had available. The NC3TF purchased a copy of an Adobe Systems product as well.

The NC3TF met with Autodesk and Adobe Systems and confirmed that the software was actually "trial" versions which had had a program added to the CD to override the security features of the trial version, thus making them fully functioning software.

After another undercover buy, and surveillance, the suspect's home was identified. A search warrant was later served on his home where 100s of copies of Autodesk and Adobe Systems programs were located.

The case has been referred to the State Attorney Generals Office for prosecution because the case involved multiple jurisdictions.

COMMENTS

"There are a number of reasons why our agency appreciates being a member of NC3TF. We like the fact that the resources of NC3TF are available to Walnut Creek. I personally appreciate the experience our investigator assigned to the task force receives. It will make him a much better detective. I also know that the professional contacts anyone assigned to NC3TF makes are invaluable throughout their law enforcement career. Additionally, NC3TF works on high tech crimes that invariably cross into several jurisdictions and a task force approach is the most effective way to deal with these types of cases."

Joel H. Bryden
Chief of Police, City of Walnut Creek

"The Sonoma County District Attorney's Office has benefited from the High Tech Task Force by providing forensic computer exams and expert testimony in Court describing their findings in child pornography cases.

The forensic exam of a computer requires significant training and expertise, while the presentation requires an expert who can present this technical information to the jury in an understandable manner. This digital evidence is a powerful tool for prosecutors and having the High Tech Task Force available to provide expert investigation and testimony is imperative."

Stephan Passalacqua
Sonoma County District Attorney

"From the on-set the Vallejo Police Department has been a participating agency in NC3TF. Early on our department has recognized the importance and value that these task forces provide throughout the state. With that we were eager to commit the necessary personnel to combat both high technology and identity theft crimes that as an organization we could not properly investigate on our own. Having NC3TF in our region has afforded the department to send our officers to the task force and receive the highly specialized training that comes with being a task force partner. In addition the detectives at our department often reach out to NC3TF for assistance in our own investigations that has proven to be invaluable."

Lt. Ken Weaver
Vallejo Police Department

SOUTHERN CALIFORNIA HIGH TECH TASK FORCE (SCHTTF)

Lead Agency: ***Los Angeles County Sheriff's Department***

SCHTTF is represented by the following three counties:

- Los Angeles
- Orange
- Ventura

Through a common memorandum of understanding, **SCHTTF** is comprised of participants from the following agencies:

- Bureau of Immigration and Customs Enforcement (ICE)
- California Department of Motor Vehicles
- California Department of Social Security
- California Highway Patrol
- Culver City Police Department
- Federal Bureau of Investigations (FBI)
- Glendale Police Department
- Los Angeles City Attorney's Office
- Los Angeles County District Attorney's Office
- Los Angeles County Sheriff's Department
- Los Angeles Police Department
- Orange County Sheriff's Department
- Oxnard Police Department
- Simi Valley Police Department
- United States Postal Service
- United States Secret Service
- Ventura County District Attorney's Office
- Ventura County Sheriff's Department
- Ventura Police Department

CASE PROFILES

A local school district contacted SCHTTF requesting assistance with the unlawful intrusion of their data network. SCHTTF determined a very sophisticated intrusion occurred using a technique called: "Man in the Middle Attack." The hacker used his personal computer to hack into the school district's router. He then re-directed the entire district's emails through his own server saving information onto it, and then exporting the emails back to the district. The district was unaware of the activity until complaints were received that the Internet connections were extremely slow. The investigation moved forward after discovering the source of the IP address used in the hacking. That led to subject interviews, preparation of search warrants, collection of evidence, and identification of suspects. The investigators also learned that the suspects were members of a hacking group, whose purpose is to exploit large corporate and governmental networks. The intrusion created severe network interruptions, causing the district numerous IT hours to rectify the damage. During the intrusion, suspects were collecting data packets associated with payroll documentation for the school district employees.

The Recording Industry Association of America contacted the Southern California High Tech Task Force regarding copy right violations against Association members. The suspect company is supplying various bars with juke boxes containing digital music in direct violation of copy right laws. The manufacturer of the juke boxes was identified as well as the suspected businesses operating in different counties in southern California. The fact that California has no enforceable law created an investigative challenge. The Task Force environment allowed the investigator to solicit federal prosecutors for assistance. Federal search warrants were eventually served and juke boxes containing the materials were seized.

Lowes stores reported that identity theft thieves took possession of over \$100,000 in fraudulently obtained merchandise. SCHTTF identified the primary suspect and established a controlled delivery of purchased items. The suspect accepted delivery and was arrested. Search warrants were served at two residences.

An elaborate skimming operation targeted gas pumps in California, Texas, Florida, Nevada, Pennsylvania, and New York. The operation netted the fraudsters over 1 million dollars. SCHTTF identified two suspects, who were arrested. A search of their residence led to the discovery of 10,000 victim profiles, a skimming operation, and a credit card manufacturing plant. The assigned Task Force prosecutor filed 56 Felony fraud related counts against the suspects.

SCHTTF arrested a probationer, who was placed on probation following a prior identity theft conviction, and his associate after discovering that he and the associate were involved in a counterfeiting and credit card manufacturing operation. Four luxury vehicles valued in excess of \$500,000 were confiscated along with firearms. Credit card manufacturing equipment valued at approximately \$65,000 was also confiscated.

SCHTTF investigators conducted a sting operation at a Circuit City store and arrested a couple involved in the counterfeiting of Green Dot Visa gift cards. A total of 550 gift cards were recovered each with a loaded credit value of \$10,000 (\$5,500,000). The cards were re-encoded with information from the targeted identity theft victims.

SACRAMENTO VALLEY HI-TECH CRIMES TASK FORCE (SVHTCTF)

Lead Agency: ***Sacramento County Sheriff's Department***

SVHTCTF is represented by the following seven counties:

- | | |
|-----------------|---------------|
| • El Dorado | • San Joaquin |
| • Merced | • Stanislaus |
| • Placer | • Yolo |
| • Plumas County | • Yuba County |
| • Sacramento | |

Through a common memorandum of understanding, **SVHTCTF** is comprised of participants from the following agencies:

- | | |
|---|--|
| • Bureau of Immigration and Customs Enforcement (ICE) | • Modesto Police Department |
| • California Department of Insurance | • Placer County District Attorney's Office |
| • California Department of Justice | • Placer County Sheriff's Department |
| • California Department of Motor Vehicles | • Plumas County Sheriff's Department |
| • California Highway Patrol | • Rocklin Police Department |
| • California State Attorney General's Office | • Roseville Police Department |
| • California State Controller's Office | • Sacramento County Probation Dept. |
| • Ceres Police Department | • Sacramento County District Attorney's Office |

- Citrus Heights Police Department
- Crescent City Police Department
- Davis Police Department
- El Dorado County Sheriff's Department
- Elk Grove Police Department
- Escalon Police Department
- Federal Bureau of Investigation (FBI)
- Folsom Police Department
- Lodi Police Department
- Manteca Police Department
- Marysville Police Department
- Merced Police Department
- Merced County Sheriff's Department
- Sacramento Police Department
- Sacramento County Sheriff's Department
- San Joaquin County Sheriff's Department
- Solano County Sheriff's Department
- Stanislaus County District Attorney's Department
- Stanislaus County Sheriff's Department
- Tracy Police Department
- Turlock Police Department
- United States Attorney's Office
- United States Postal Inspection Services
- United States Secret Service
- USDA Forest Service
- Woodland Police Department

CASE PROFILES

In March 2009, SVHTCTF started an investigation into the Suspect and his business for online business fraud. Fifty to sixty complaints were submitted to various entities including IC3, the Sacramento Better Business Bureau, California Department of Public Health, the Federal Trade Commission, the Sacramento Multiple Sclerosis Center of Sacramento, and the Sacramento Valley Hit-Tech Crimes Task Force. The victims were located across the country. Some were reporting as little as \$375 loss to as much as \$2,004 loss. The victims were elderly and/or disabled. Several victims are disabled American Veterans.

The suspect's business was a real business located in Sacramento. The suspect accepted orders and payment for scooters and other accessories but did not ship the purchased items. The suspect has refused to issue refunds at the victim's request. The suspect also has refused to cooperate with the California Department of Public Health and the Sacramento Better Business Bureau to settle the numerous complaints against him and his business.

The California Department of Public Health, Food and Drug Branch have cited the suspect and his business numerous times for health and safety and Sacramento City Code violations between January 22, 2007 and December 23, 2008. The suspect has never satisfied the conditions to remove those violations. He was also found to have operated without a HMDR License which is required in order to sell medical equipment in the State of California. The suspect has since vacated the Sacramento location; and according to the Better Business Bureau, has a forwarding address in Davies, Florida.

The estimated aggregate loss is \$40,000.

SVHTCTF investigated an intellectual property theft case with Hewlett Packard of Roseville being the victim. Investigators from Hewlett Packard reported to the Task Force that a current employee of theirs along with an accomplice had stolen hardware and proprietary software belonging to HP. The total loss was estimated to be \$100,000.

A search warrant was served at the house of one of the suspects. A majority of the property was located at the residence, recovered, and subsequently returned to Hewlett Packard. Two suspects were taken into custody. Both of them admitted to the crime and gave incriminating statements to SVHTCTF. This case was an excellent example of a regional operation. Investigators from Placer

County, Roseville Police and Hewlett Packard were involved in the investigation. This case will be tried in Placer County.

On March 26, 2009, SVHTCTF identified and arrested two suspects who are believed to be responsible for multiple thefts at 24-Hour Fitness locations throughout the Sacramento area. These thefts occurred between November 2008 and March 2009. At this time, SVHTCTF has identified over 40 victims in the investigation.

This husband and wife suspect team would target people while they were exercising. The female suspect would enter the gym using a stolen membership card, while the male suspect remained outside as a look-out. Once inside, the suspect would proceed directly to the locker room where she would break into and steal items from lockers. These items were usually purses or wallets containing credit cards and checks, gym membership cards, and car keys. The suspects would use the stolen financial instruments to commit identity theft. This included using the stolen membership cards to re-enter other 24 Hour Fitness locations and repeating the process.

A search of the suspect's residence produced over 60 purses and wallets, victim's car keys, and cell phones. SVHTCTF is now in the process of working with 24-Hour Fitness to determine if there are additional victims and return as much of the stolen property as possible.

Between 8-12-08 and 9-9-08 the suspect entered Golden 1 Credit Union branches located in Sacramento County on at least seventeen separate occasions and fraudulently accessed four individual accounts. The suspect cashed numerous fraudulent checks against the accounts and withdrew cash. Golden1 has sustained a loss of \$37,168.78 as a result of the fraudulent activity. The suspect was captured by Golden1 surveillance cameras conducting the fraudulent transactions. The person depicted in the surveillance photos appears to be the suspect. On 9-9-08 the suspect was arrested while attempting to cash a check against one of the four victim accounts. The suspect was out on bail for an unrelated case when he committed the above crimes.

COMMENTS

"Being a member of the Sacramento Valley Hi-Tech Crimes Task Force has allowed our department to better serve the citizens of our community. The sharing of resources has helped tremendously in making the most efficient use of our limited budget."

Wallace C. Fullerton,
Chief of Police, Marysville Police Department

"Nothing affects the quality of life in a community more than the quality of its Law Enforcement. We are pleased that we can assist and support the Sacramento Valley High Technology Task Force in maintaining and improving it's excellence with technology crime investigation throughout the Sacramento Valley region."

Mike Menz
Chief Investigator, Hewlett Packard

"The Sacramento Hi-Tech Crimes Task force has played a critical role in our efforts to protect our guest, team members and profits – which in turn protects the tax revenues important to maintain the high standards of service in our community. The task force has been a key partner for my team in resolving complex investigations that have significantly impacted Target. There have been too many

collaborative investigations to list but I will highlight one. Because of the responsiveness, agility and proficiency of the Hi-Tech Crimes task force, they were able to help us by resolving a credit card case which impacted Target for approximately \$300,000.”

Marc Rojas
Chief Investigator, Target

“Working in loss prevention for over 13 years has taught me how important specialty task force law enforcement teams are in working with retail to identify, investigate and resolve specialty crimes. There are a substantial amount of persons using non-conventional means to commit crimes ranging from identity theft, credit card, and check fraud. Most of these persons specifically target access points of pay and use technology to by-pass typical retail safe-guards against fraud. Specialty teams, such as the Identity Task Force, are a vital element in bringing these types of crimes to justice. Walmart has a long history of working with Sacramento County Identity Task Force. Our collaborative efforts have yielded several arrest of subjects that with out specialty investigative teams both within law enforcement and Walmart may not had been possible.”

Lee Frasier,
Walmart Asset Protection Investigations

CALIFORNIA DISTRICT ATTORNEY’S ASSOCIATION

The California District Attorney’s Association (CDAA) employs HTTAP funds to continue developing and presenting its high tech crime prosecution training program. CDAA’s efforts augment and enhance statewide efforts to combat on-line fraud, identity theft and other crimes perpetrated with the use of high technology by providing task force personnel and others with the specialized training needed to effectively address the evolving and complex problems often posed by these offenses.

CDAA’s program provides training to prosecutors and law enforcement officers from all California counties. The training is multi-disciplinary and targets the successful investigation, apprehension, and prosecution of criminal organizations, networks, and individuals involved in high technology and computer-based crimes. CDAA complements this program with an on-going series of publications and legal updates.

CDAA’s HTTAP funds support the following specific activities:

- Development and publication of CDAA’s high technology crimes newsletter, ***Firewall***, which highlights emerging issues, relevant legislative updates, pertinent court cases and upcoming training opportunities.
- Production and distribution of California’s first high tech crime prosecution practice guide, ***Investigation and Prosecutions of High Tech Crimes***. Overwhelming demand for the printed manual has necessitated the publication of the manual on CD-ROM.
- Development and maintenance of online resources including:
 - A PowerPoint and audio library available to all California prosecutors;
 - A brief bank which currently houses over 200 high-technology briefs, points and authorities, and court cases;
 - An expert witness database containing 688 documents including transcripts, articles, briefs, and curricula vita on over 100 different experts;
 - A project website which provides all California prosecutors with updated resources guides and links to the various other sources mentioned above;

- Providing *ad hoc* technical and legal assistance to California prosecutors and investigators who must respond to unforeseen high tech crime problems in court and in the field.
- Providing training to over 134 prosecutors throughout the state of California at five different training courses. Three of those trainings included “hands-on” interaction (thanks to the cooperative use of a mobile computer lab provided by California Department of Justice’s Advanced Training Center).
- CDAA has also initiated “Webinar” training sessions for prosecutors who cannot attend in person. These high-quality and informative trainings are provided in “real time” and delivered to participating student’s individual desktops.

A total of \$286,343 was awarded to CDAA in furtherance of these activities. This amount includes a 25 percent match of \$59,880.

DOJ DEPUTY ATTORNEY GENERAL * IDENTITY THEFT SUPPORT

There are five Deputy Attorneys General (DAGs) and one Special Agent assigned to support the High Technology Identity Theft Program which is administered through the OES. One DAG is assigned to support each of the five task forces.

The DAGs duties include: (1) Prosecution support to the five task forces; (2) Development and delivery of training programs to law enforcement and the public; (3) Legal and prosecution support to rural counties; (4) Coordination of out-of-state investigation request; and (5) State agency legal and prosecution support.

During the 2009 fiscal year the DAGs initiated 2 investigations, filed 2 indictments and 22 criminal complaints, convicted 63 defendants, and sentenced 25 defendants. The DAGs also provided 27 trainings on identify theft issues for law enforcement and the public.

Funds have been allocated to DOJ to create the HTTAP-Identity Theft Support Project, which is part of the Special Crimes Unit in the Office of the Attorney General. A total of \$339,440 was awarded to DOJ in furtherance of the DAG Identity Theft Support Project.

DOJ DATABASE

One aspect of the DOJ portion of the HTTAP Program is the development and maintenance of statewide databases for use in developing and distributing intelligence information to participating law enforcement agencies. These databases are accessible via the Internet, using a secure digital token.

The **Case Information Management System** (CIMS) is an automated database that facilitates management of case information for agents, supervisors, and support staff. CIMS provides a central repository for case data which can be shared among all the participating Task Forces. CIMS can be utilized to create reports, operational plans, and capture statistical data. The data contained within the application does not have to be 28CFR compliant.

DOJ has been working with the Task Forces to export data from their existing databases into the CIMS. Since some of the Task Forces are mandated to enter data into other databases, setting up the export process negates the need for dual entry. Additionally, DOJ has modified the existing CIMS database in order to meet the statistical and reporting needs of the Task Forces.

Below is a summary of cases entered in the CIMS database

Task Force	Number of Cases Entered
CATCH	29
REACT	1
Sacramento	112
Southern California Regional	8

The **California State Intelligence Index (CSII)** is an automated database that allows law enforcement agencies to share intelligence information. CSII has been designed to allow users to store, inquire against, and analyze intelligence information. Once information entered into CIMS is determined to have a criminal predicate (28CFR compliant), it can be stored to CSII.

To date, no Task Force information has been submitted to CSII.

The majority of Task Force members have been trained on the CIMS application.

Below is a summary of training provided in 2009

Task Force	Training Date	Number of Attendees
CATCH	05/06/09	20
REACT	05/27/09 & 05/28/09	20
Sacramento	02/24/09 & 02/25/09	29
Sacramento	03/17/09	3
Sacramento	05/12/09	5
ID NORTH/SOUTH	02/04/09 & 02/05/09	19
ID NORTH/SOUTH	05/07/09	3
SOCAL	02/04/09 & 02/05/09	9
SOCAL	05/07/09	2
NC3TF	TBD	TBD

The remaining members are scheduled to attend training in 2010. CIMS refresher and CSII training will be provided on an as-needed basis. Due to budget constraints and DOJ travel restrictions, all training will be held in Sacramento.

The DOJ is dedicated to continued support of the program to ensure the databases meet the needs of the Task Forces.

DOJ ADVANCED TRAINING CENTER

The DOJ Advanced Training Center (ATC) has in place an interagency agreement with the OES.

The goals of this agreement are:

- To provide additional high technology investigation training classes to California peace officers, especially personnel assigned to the five regional task forces.
- To provide advanced training in the area of computer forensics.
- To provide equipment to personnel who conduct computer forensic examinations.

The primary objectives are:

- To create a program that would continuously update the curriculum for teaching high technology investigation techniques and computer forensics.
- To base the changes on trends in crime, law and technology.
- To create a program (a series of classes) that would train an investigator from a 'basic introduction' to high technology crimes, to an advanced level of computer forensic investigation competency.
- To develop the classes necessary to complete this series.
- To test the students on learned skills and knowledge of computer crime investigations.

HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE

The High Technology Crime Advisory Committee (HTCAC) was established concurrently with the HTTAP Program. The purpose of the committee is to provide strategic oversight to the program and conduct planning in response to high technology crime in California. This committee includes representatives of the following agencies/organizations:

- (1) A designee of the California District Attorneys Association.
- (2) A designee of the California State Sheriffs Association.
- (3) A designee of the California Police Chiefs Association.
- (4) A designee of the Attorney General.
- (5) A designee of the California Highway Patrol.
- (6) A designee of the High Technology Crime Investigation Association.
- (7) A designee of the California Emergency Management Agency.
- (8) A designee of the American Electronic Association to represent California computer system manufacturers.
- (9) A designee of the American Electronic Association to represent California computer software producers.
- (10) A designee of CTIA--The Wireless Association.
- (11) A representative of the California Internet industry.
- (12) A designee of the Semiconductor Equipment and Materials International.
- (13) A designee of the California Cable & Telecommunications Association.
- (14) A designee of the Motion Picture Association of America.
- (15) A designee of the California Communications Associations (CalCom).
- (16) A representative of the California banking industry.
- (17) A representative of the Office of Information Security and Privacy Protection.
- (18) A representative of the Department of Finance.
- (19) A representative of the State Chief Information Officer.
- (20) A representative of the Recording Industry of America.
- (21) A representative of the Consumers Union.

HTCAC ACTIVITIES

During the reporting period the HTCAC has addressed various areas of public safety concerns for the citizens of California. As noted above, California loses millions of dollars to criminals via counterfeiting and piracy of technical, education, business and entertainment industry software and hard goods. In addition to providing direction and guidance at quarterly HTCAC meetings (which are attended by personnel from the five task forces, general law enforcement, the industries represented by the Committee, educators and the general public), HTCAC members provided insight, technical assistance and practical support for initiatives to stem the tide of technology facilitated lawlessness.

One such area has been the effort to reinstitute concurrent jurisdiction among the states and the federal government in the area of enforcement of copyright law violations. Currently the tide of crime in this area has far outstripped the resources of the federal government to effectively prosecute the breadth of this crime allowing the theft of hundreds of millions of dollars from California corporations to continue with virtual impunity.

The HTCAC consistently reviews the standards and goals of the task forces and evaluates the practicality and applicability of them in light of changing technologies, crime patterns and societal norms. Periodically the HTCAC recommends modifications for the managing state agency (now Cal-EMA) to implement in order to maintain the effectiveness of the task forces.

As representatives of the high technology industries, HTCAC members facilitate solutions to and help manage the tension between the industries' interest in protecting their trade secrets and stock value by avoiding public disclosures inherent in the criminal justice process and the need to cooperate with law enforcement for effective policing of those who would do harm to the industry (both from without and within) costing the state and its citizens millions of dollars in losses.

HTCAC committee members also facilitate interaction between law enforcement as represented on the committee and the high technology industry through appearances at key meetings and conferences sponsored by organizations such as TechNet (a bipartisan, political network of CEOs and Senior Executives that promotes the growth of technology and the innovation economy).

HTCAC members committed to facilitating productive exchanges between legislators, the high technology industry and law enforcement to secure means of sustainable funding for the task forces with a view to emphasizing the value, both financial and societal, to the industry and government in keeping the task forces viable.

During the reporting period in order to keep the program viable in light of technological changes and evolving crime patterns, the HTCAC has engaged in a review and revision of the initial HTTAP Strategy which was originally adopted February 17, 1999 and last revised March 11, 2004.

The HTCAC also monitors the development and maintenance of a trust account facilitated by the CDAA for the benefit of the task forces. The account was created to accept monies from settlements in high-tech cases and other sources outside the normal funding pattern.

At most quarterly meetings the HTCAC is given a presentation by one of the task forces on a case and/or shareable intelligence, so that they can pass that information on to industry personnel. This trust relationship fosters interaction between the industry and law enforcement to better protect the public.

The HTCAC meetings also provide a forum for the direct dissemination of information such as the status of production of new training materials and programs and sources for assistance in getting such implemented. Examples are the statewide ID Theft Manual and the California Attorney General's

e-mail piracy training CD. Other examples are the development of regional secure wide-area networks that allow case investigators and prosecutors to search duplicate copies of seized digital evidence themselves, thereby reducing the demands being made on forensic examiners. These programs allow the examiners to concentrate on higher level functions and will reduce backlogs that would otherwise occur in the forensic labs.

The HTCAC monitors and reviews pending legislation each quarter through the auspices of the CDAA member and provides suggestions, support for and opposition to various bills in an effort to keep California on a track that encourages continuation of its leading status in the fight against cyber crime and identity theft.

Finally, the HTCAC has provided the forum through which the task forces have been able to work out the details of and finally adopt a functional crime database system to maintain compliance with their legislative mandate.

CONCLUSION

The funding for the High Technology Task Force is only assured through the 2010-2011 fiscal year. The state of California must have a force to counter the high tech crimes committed against our citizens and industries. Legislative action is required to assure continuation of the actions taken to date. A positive proactive solution will allow the task force members to continue their work on behalf of our citizens and industries. New task force members can be recruited and trained and the work will continue without interruption. We know that the future of California is important to all of us and protection against high tech crime and identity theft is a valuable component of our future.

APPENDIX A

California Penal Code Sections 13848-13848.6

Penal Code 13848 Legislative intent; prevention of technology-related crimes

(a) It is the intent of the Legislature in enacting this chapter to provide local law enforcement and district attorneys with the tools necessary to successfully interdict the promulgation of high technology crime. According to the federal Law Enforcement Training Center, it is expected that states will see a tremendous growth in high technology crimes over the next few years as computers become more available and computer users more skilled in utilizing technology to commit these faceless crimes. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which is the target of a criminal act.

(b) Funds provided under this program are intended to ensure that law enforcement is equipped with the necessary personnel and equipment to successfully combat high technology crime which includes, but is not limited to, the following offenses:

(1) White-collar crime, such as check, automated teller machine, and credit card fraud, committed by means of electronic or computer-related media.

(2) Unlawful access, destruction of or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, or unauthorized disclosure of data stored within those computers and networks.

(3) Money laundering accomplished with the aid of computer networks or electronic banking transfers.

(4) Theft and resale of telephone calling codes, theft of telecommunications service, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.

(5) Software piracy and other unlawful duplication of information.

(6) Theft and resale of computer components and other high technology products produced by the high technology industry.

(7) Remarking and counterfeiting of computer hardware and software.

(8) Theft of trade secrets.

(c) This program is also intended to provide support to law enforcement agencies by providing technical assistance to those agencies with respect to the seizure and analysis of computer systems used to commit high technology crimes or store evidence relating to those crimes.

Penal Code 13848.2 High Technology Theft Apprehension and Prosecution Program; establishment; funding

(a) There is hereby established in the California Emergency Management Agency a program of financial and technical assistance for law enforcement and district attorneys' offices, designated the High Technology Theft Apprehension and Prosecution Program. All funds allocated to the California Emergency Management Agency for the purposes of this chapter shall be administered and disbursed by the Secretary of Emergency Management in consultation with the High Technology Crime Advisory

Committee as established in Section 13848.6 and shall to the extent feasible be coordinated with federal funds and private grants or private donations that are made available for these purposes.

(b) The Secretary of California Emergency Management is authorized to allocate and award funds to regional high technology crime programs which are established in compliance with Section 13848.4.

(c) The allocation and award of funds under this chapter shall be made on application executed by the district attorney, county sheriff, or chief of police and approved by the board of supervisors for each county that is a participant of a high technology theft apprehension and prosecution unit.

Penal Code 13848.4 Expenditure of allocated funds

(a) Moneys allocated for the High Technology Theft Apprehension and Prosecution Program pursuant to subdivision (b) of section 13821 shall be expended to fund programs to enhance the capacity of local law enforcement and prosecutors to deter, investigate, and prosecute high technology related crimes. After deduction of the actual and necessary administrative costs referred to in subdivision (f), the funds shall be expended to fund programs to enhance the capacity of local law enforcement, state police, and local prosecutors to deter, investigate, and prosecute high technology related crimes. Any funds distributed under this chapter shall be expended for the exclusive purpose of deterring, investigating, and prosecuting high technology related crimes.

(b) Up to 10 percent of the funds shall be used for developing and maintaining a statewide database on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies. In addition, the Secretary of California Emergency Management may allocate and award up to 5 percent of the funds available to public agencies or private nonprofit organizations for the purposes of establishing statewide programs of education, training, and research for public prosecutors, investigators, and law enforcement officers relating to deterring, investigating, and prosecuting high technology related crimes. Any funds not expended in a fiscal year for these purposes shall be distributed to regional high technology theft task forces pursuant to subdivision (b).

(c) Any regional task force receiving funds under this section may elect to have the Department of Justice administer the regional task force program. The department may be reimbursed for any expenditure incurred for administering a regional task force from funds given to local law enforcement pursuant to subdivision (b).

(d) The California Emergency Management Agency shall distribute funds to eligible agencies pursuant to subdivision (b) in consultation with the High Technology Crime Advisory Committee established pursuant to Section 13848.6.

(e) Administration of the overall program and the evaluation and monitoring of all grants made pursuant to this chapter shall be performed by the California Emergency Management Agency.

Penal Code 13848.6. High Technology Crime Advisory Committee; disbursing funds

(a) The High Technology Crime Advisory Committee is hereby established for the purpose of formulating a comprehensive written strategy for addressing high technology crime throughout the state, with the exception of crimes that occur on state property or are committed against state employees, and to advise the California Emergency Management Agency on the 35 appropriate disbursement of funds to regional task forces.

(b) This strategy shall be designed to be implemented through regional task forces. In formulating that strategy, the committee shall identify various priorities for law enforcement attention, including the following goals:

(1) To apprehend and prosecute criminal organizations, networks, and groups of individuals engaged in the following activities:

(A) Theft of computer components and other high technology products.

(B) Violations of Penal Code Sections 211, 350, 351a, 459, 496, 537e, 593d, 593e, 653h, 653s, and 635w.

(C) Theft of telecommunications services and other violations of Penal Code Sections 502.7 and 502.8.

(D) Counterfeiting of negotiable instruments and other valuable items through the use of computer technology.

(E) Creation and distribution of counterfeit software and other digital information, including the use of counterfeit trademarks to misrepresent the origin of that software or digital information.

(F) Creation and distribution of pirated sound recordings or audiovisual works or the failure to disclose the origin of a recording or audiovisual work.

(2) To apprehend and prosecute individuals and groups engaged in the unlawful access, destruction, or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wire line communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, and unauthorized disclosure of data stored within those computers.

(3) To apprehend and prosecute individuals and groups engaged in the theft of trade secrets.

(4) To investigate and prosecute high technology crime cases requiring coordination and cooperation between regional task forces and local, state, federal, and international law enforcement agencies.

(c) The Secretary of California Emergency Management shall appoint the following members to the committee:

(1) A designee of the California District Attorneys Association.

(2) A designee of the California State Sheriffs Association.

(3) A designee of the California Police Chiefs Association.

(4) A designee of the Attorney General.

(5) A designee of the California Highway Patrol.

(6) A designee of the High Technology Crime Investigation Association.

(7) A designee of the California Emergency Management Agency.

(8) A designee of the American Electronic Association to represent California computer system manufacturers.

(9) A designee of the American Electronic Association to represent California computer software producers.

(10) A designee of CTIA – The Wireless Association.

(11) A representative of the California Internet industry.

(12) A designee of the Semiconductor Equipment and Materials International.

(13) A designee of the California Cable & Telecommunications Association.

(14) A designee of the Motion Picture Association of America.

(15) A designee of the California Communications Associations (CalCom).

(16) A representative of the California banking industry.

(17) A representative of the Office of Information Security and Privacy Protection.

- (18) A representative of the Department of Finance.
- (19) A representative of the State Chief Information Officer.
- (20) A representative of the Recording Industry of America.
- (21) A representative of the Consumers Union.

(d) The Secretary of California Emergency Management shall designate the Chair of the High Technology Crime Advisory Committee from the appointed members.

(e) The advisory committee shall not be required to meet more than 12 times per year. The advisory committee may create subcommittees of its own membership, and each subcommittee shall meet as often as the subcommittee members find necessary. It is the intent of the Legislature that all advisory committee members shall actively participate in all advisory committee deliberations required by this chapter. Any member who, without advance notice to the Secretary of California Emergency Management and without designating an alternative representative, misses three scheduled meetings in any calendar year for any reason other than severe temporary illness or injury (as determined by the secretary) shall automatically be removed from the advisory committee. If a member wishes to send an alternative representative in his or her place, advance written notification of this substitution shall be presented to the executive director. This notification shall be required for each meeting the appointed member elects not to attend. Members of the advisory committee shall receive no compensation for their services, but shall be reimbursed for travel and per diem expenses incurred as a result of attending meetings sponsored by the California Emergency Management Agency.

(f) The Secretary of California Emergency Management, in consultation with the High Technology Crime Advisory Committee, shall develop specific guidelines and administrative procedures for the selection of projects to be funded by the High Technology Theft Apprehension and Prosecution Program, which guidelines shall include the following selection criteria:

(1) Each regional task force that seeks funds shall submit a written application to the committee setting forth in detail the proposed use of the funds.

(2) In order to qualify for the receipt of funds, each proposed regional task force submitting an application shall provide written evidence that the agency meets either of the following conditions:

(A) The regional task force devoted to the investigation and prosecution of high technology related crimes is comprised of local law enforcement and prosecutors, and has been in existence for at least one year prior to the application date.

(B) At least one member of the task force has at least three years of experience in investigating or prosecuting cases of suspected high technology crime.

(3) Each regional task force shall be identified by a name that is appropriate to the area that it serves. In order to qualify for funds, a regional task force shall be comprised of local law enforcement and prosecutors from at least two counties. At the time of funding, the proposed task force shall also have at least one investigator assigned to it from a state law enforcement agency. Each task force shall be directed by a local steering committee composed of representatives of participating agencies and members of the local high technology industry.

(4) The California High Technology Crimes Task Force shall be comprised of each regional task force developed pursuant to this subdivision.

(5) Additional criteria that shall be considered by the advisory committee in awarding grant funds shall include, but not be limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

- (B) The number of high technology crime cases investigated in the prior year.
- (C) The number of victims involved in the cases filed.
- (D) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, or corporations, as a result of the high technology crime cases filed, and those under active investigation by that task force.

(6) Each regional task force that has been awarded funds authorized under the High Technology Theft Apprehension and Prosecution Program during the previous grant-funding cycle, upon reapplication for funds to the committee in each successive year, shall be required to submit a detailed accounting of funds received and expended in the prior year in addition to any information required by this section. The accounting shall include all of the following information:

- (A) The amount of funds received and expended.
- (B) The use to which those funds were put, including payment of salaries and expenses, purchase of equipment and supplies, and other expenditures by type.
- (C) The number of filed complaints, investigations, arrests, and convictions that resulted from the expenditure of the funds.

(g) The committee shall annually review the effectiveness of the California High Technology Crimes Task Force in deterring, investigating, and prosecuting high technology crimes and provide its findings in a report to the Legislature and the Governor. This report shall be based on information provided by the regional task forces in an annual report to the committee which shall detail the following:

(1) Facts based upon, but not limited to, the following:

- (A) The number of high technology crime cases filed in the prior year.
- (B) The number of high technology crime cases investigated in the prior year.
- (C) The number of victims involved in the cases filed.
- (D) The number of convictions obtained in the prior year.
- (E) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations, and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained.

(2) An accounting of funds received and expended in the prior year, which shall include all of the following:

- (A) The amount of funds received and expended.
- (B) The uses to which those funds were put, including payment of salaries and expenses, purchase of supplies, and other expenditures of funds.
- (C) Any other relevant information requested.

APPENDIX B

HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE MEMBERS MEMBER / ADDRESS/TELEPHONE ORGANIZATION REPRESENTED

William E. Eyres – Chair Governor’s Office of Emergency Services

8831 Berta Ridge Court

Prunedale, CA 93907

831-663-3695

eyres@montereybay.com

Saul Arnold – Vice Chair Semiconductor Equipment and Materials International

Corporate Counsel, Legal Services

Law Department

Applied Materials, Inc.

3050 Bowers Ave. M/S 2062

P.O. Box 58039

Santa Clara, CA 95054

408-563-4590

408-986-2836 (fax)

saul_arnold@amat.com

Craig Beuhler California Department of Justice

Bureau Chief

California Department of Justice

Bureau of Investigation and Intelligence

1102 Q Street, Room 6050

Sacramento, CA 95814

916-319-9282

916-319-9440 (fax)

Craig.buehler@doj.ca.gov

Joe Camicia State Chief Information Officer

Chief of Staff

Office of the Chief Information Officer

1325 J Street, Suite #1600

Sacramento, CA 95814

916-319-9223

Joe.camicia@cio.ca.gov

Todd Chadd California Highway Patrol

Assistant Chief

Information Management Division

California Highway Patrol

2555 First Avenue

Sacramento, CA 95818

916-647-7171

TChadd@chp.ca.gov

Jack Christin, Jr. California Internet Industry E-Bay/PayPal

Trust & Safety Counsel

eBay, Inc.

2145 Hamilton Avenue

San Jose, CA 95125

408-376-5145

408-376-7517 (fax)

ichristin@ebay.com

Mark Domnauer American Electronic Association

Director, Global Safety and Security (Calif. Computer Software Producers)

Adobe Systems Incorporated

345 Park Avenue, MS A09-406

San Jose, CA 95110

408-536-4049

408-536-6616 (fax)

domnauer@adobe.com

Donald Duggan California Banking Industry

Senior Executive Vice President & CIO

Bank of the West

180 Montgomery Street, 25th Floor

San Francisco, CA 94104

415-765-4883

415-765-4858 (fax)

donald.duggan@bankofthewest.com

Merle (Bud) Frank California District Attorneys Assoc.

Deputy District Attorney

County of Santa Clara

County Government Center, West Wing

70 West Hedding Street

San Jose, CA 95110

408-792-2469

408-279-8742 (fax)

Bfrank@da.sccgov.org

Margaret Felts California Communications Assoc.

President, California Communications Association

1321 Howe Avenue, Suite 201

Sacramento, CA 95825

916-567-6702

916-922-3648

mcf@calcom.ws

Brian Gurwitz Recording Indust. Assoc. of America

Regional Counsel, Anti-Piracy Legal Affairs

Recording Industry Association of America

10842 Noel Street, #106

Los Alamitos, CA 90720

714-236-0830

714-236-0930 (fax)

bgurwitz@riaa.com

Jim Cooper, Captain California State Sheriff's Assoc.

Sacramento County Sheriff's Department
3720 Dudley Boulevard
McClellan, CA 95652
916-874-3007
916-874-3006 (fax)
jcooper@sacsheriff.com

Steven Lund American Electronic Association

Director, Corporate Security (Calif. Computer Syst. Manufacturers)
Intel Corporation
4500 S. Dobson Road, OC4-35
Chandler, AZ 85248
480-715-5036
Steven.j.lund@intel.com

Rocky P. McCants Calif. Cable & Telecommunications Association

Regional Security Director
Comcast Cable
12647 Alcosta Blvd., Suite 200
San Ramon, CA 94583
925-973-7074
925-901-0231 (fax)
Rocky_mccants@cable.comcast.com

John McMullen, Lt. (Retired)

Santa Clara Co. Dist. Attorney's Office
Bureau of Investigation
High Technology Crime Unit
70 West Hedding Street, West Wing
San Jose, CA 95110
408-210-9508 (cell)
jmcmullen@da.sccgov.org

Joanne McNabb Calif. Office of Information & Privacy Protection

Chief, Office of Privacy Protection
California Office of Information & Privacy Protection
1325 J Street, Suite 1650
Sacramento, CA 95814
916-323-7301
916-323-7299 (fax)
Joanne.McNabb@OISPP.ca.gov

Bruce Muramoto California Police Chiefs Association

Chief of Police
City of Winters
318-A First Street
Winters, CA 95694
530-795-2261 (ext. 121)
530-795-3921 (fax)
Bruce.muramoto@winterspolice.org

Jennifer Osborn California Department of Finance

Principal Program Budget Analyst
Corrections/General Government Unit
Department of Finance
915 L Street, 8th Floor
Sacramento, CA 95814
916-45-8913

Jennifer.osborn@dof.ca.gov

Kevin Suh Motion Picture Assoc. of America

Deputy Director
15301 Ventura Blvd., Building E
Sherman Oaks, CA 91403
818-995-6600
818-285-4408 (fax)

kevin_suh@mpaa.org

Mark Yamane (Northern California rep.) **Calif. Communications Assoc. (CalCom)**

Buck Carter (Southern California rep.) **Vacant Consumers Union**

Area Manager-Asset Protection
(Appointment pending approval)
(858) 320-5520 or (619) 518-7990

**APPENDIX C
HIGH TECHNOLOGY THEFT APPREHENSION & PROSECUTION PROGRAM
PROJECT DIRECTORS**

Gil VanAttenhoven Interagency Agreement No. 6050-8

Special Agent in Charge
Advanced Training Center
Department of Justice
11181 Sun Center Drive
Rancho Cordova, CA 95670
916-464-5591
FAX 916-464-5577
Gil.vanattenhoven@doj.ca.gov

Edward Berberian OES Grants Nos. HD08080210 and HT08080210

District Attorney
Marin County
3501 Civic Center Drive, #130
San Rafael, CA 94903
415-499-6450
707-253-4664
eberberian@co.marin.ca.us

Craig Buehler OES Grant No. HT08089504

Bureau Chief
California Department of Justice
Bureau of Investigation and Intelligence
1102 Q Street, Room 6050
Sacramento, CA 95814
916-319-9282
FAX 916-319-9440
craig.buehler@doj.ca.gov

Brandon McHugh OES Grants Nos. HD08080370 and HT08080370

Deputy District Attorney
Chief, Economic Crimes Division
San Diego County District Attorney's Office
330 W. Broadway, Suite 700
San Diego, CA 92101
619-531-3102
FAX 619-531-4481
brandon.mchugh@sdcdca.org

James Cooper, Capt. OES Grants Nos. HD08080340 & HT08090340

Sacramento County Sheriff's Department
3720 Dudley Blvd.
McClellan, CA 95652
916-874-3030
FAX 916-874-3006
jcooper@sacsheriff.com

Rich Daniels, Lt. OES Grant No. HT08090190

Los Angeles County Sheriff's Department
11515 S. Colima Rd., #M-104
Whittier, CA 90604
562-347-2602
FAX 323-415-3421
rrdaniel@lasd.org

David Hendrickson, Lt. OES Grants Nos. HD08080430 and HT08090430

County of Santa Clara District Attorney's Office
Bureau of Investigation
High Technology Crime Unit
70 West Hedding Street, West Wing
San Jose, CA 95110
408-792-2879
FAX 408-947-0692
dhenrickson@da.sccgov.org

Ron Smetana OES Grant No. HD08089504

Senior Assistant Attorney General
Special Crimes Unit
Office of the Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
415-703-5856
Ron.smetana@doj.ca.gov

W. Scott Thorpe OES Grant No. HT08081059

Chief Executive Officer
California District Attorneys Association
731 K Street, Third Floor
Sacramento, CA 95814
916-443-2017
sthorpe@cdaa.org

Ronald D. Williams, Lt. OES Grant No. HD08080190

Los Angeles County Sheriff's Department
9900 Norwalk Blvd., Suite 150A
Santa Fe Springs, CA 90670
562-347-2661
FAX 323-415-3818
rdwillia@lasd.org

APPENDIX D

HTCAC BYLAWS STATE OF CALIFORNIA BYLAWS, RULES AND PROCEDURES OF THE HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE *Adopted: June 2005* *Revised: December 2008*

ARTICLE I: NAME AND AUTHORITY

This organization, created in the State government by statutory authority, shall be known as the High Technology Crime Advisory committee – hereinafter referred to as the “Committee.”

ARTICLE II: MEMBERSHIP AND CHAIRPERSON SELECTION

Section 1.

The Committee shall include the following twenty one representatives:

- (1) A designee of the California District Attorneys Association;
- (2) A designee of the California State Sheriff’s Association;
- (3) A designee of the California Police Chief’s Association;
- (4) A designee of the California Attorney General;
- (5) A designee of the California Highway Patrol;
- (6) A designee of the High Technology Crime Investigation Association;
- (7) A designee of the California Office of Emergency Services;
- (8) A designee of the American Electronic Association to represent California computer system manufacturers;
- (9) A designee of the American Electronic Association to represent California software producers;
- (10) A designee of the CTIA – The Wireless Association;
- (11) A designee of the California Internet Industry;
- (12) A designee of the Semiconductor Equipment and Materials International (SEMI);
- (13) A designee of the California Cable Television Association;
- (14) A designee of the Motion Picture Association of America;
- (15) A designee of the California Communications Association (CalCom);
- (16) A representative of the California Banking Industry;
- (17) A representative of the California Office of Information Security and Privacy Protection;
- (18) A representative of the California Department of Finance;
- (19) A representative of the State Chief Information Officer;
- (20) A designee of the Recording Industry of America; and
- (21) A designee of the Consumers Union.

Section 2.

The chairperson of the Committee shall be selected by the Executive Director of the Office of Emergency Services from among the members of the Committee [Penal Code Section 13848.6(d)].

ARTICLE III: POWERS AND DUTIES

Section 1.

The Committee is empowered to act as the advisory board of the Office of Emergency Services in accordance with the mandates of the pertinent state acts and programs. The Committee may develop and/or modify and recommend to the Office of Emergency Services a high technology plan.

Section 2.

The Committee may develop policy recommendations for the Governor, the Legislature, the Office of Emergency Services and the local units of government on major criminal justice issues where a high technology nexus exists. To that end, the Committee understands itself to be the primary advisory board on technology-related criminal justice issues.

Its goals include:

1. Identifying current, developing and future issues involving high technology crime and criminal justice policy and procedures relevant to such issues;
2. Developing an understanding of the issues attendant to high technology crime and making conclusions that provide the foundation for recommendations to the Office of Emergency Services, the Governor and the Legislature concerning high technology crime, criminal identification, apprehension and prosecution;
3. Issuing analysis of current or pending high technology criminal justice-related legislation;
4. Assisting California's criminal justice agencies and practitioners in the effective use of resources regarding high technology crime;
5. Coordinating studies and recommendations with the Office of Emergency Services and other criminal justice agencies with a view toward isolating issues common to high technology crime and justice.

ARTICLE IV: COMMITTEE MEETINGS

Section 1.

The Committee shall meet at such intervals as necessary to carry out its duties, but no more than twelve meetings shall be held annually. Regular meetings of the Committee shall be held at least quarterly unless, in the opinion of the Committee Chair and Vice Chair, there are insufficient items of business or insufficient funds to call such quarterly or regular meetings. The Executive Secretary of the Committee shall give a minimum of ten days written advance notice to the membership of the Committee of the time and place of a regular meeting.

Section 2.

Special meetings of the Committee may be called at any time by the Committee Chair. Forty-eight hours prior notice of the time and place of such special meetings shall be given by the Chair to the members, where permitted by law.

Section 3.

Meetings shall be conducted in accordance with these bylaws and Robert's Rules of Order.

ARTICLE V: SUBCOMMITTEES AND SUBCOMMITTEE MEETINGS

Section 1.

The Committee shall have the following subcommittees:

- Strategy Subcommittee
- Bylaws Subcommittee

ARTICLE VI:

Section 2.

The Committee may recommend the creation of such subcommittees of its own membership as it deems necessary.

Section 3.

By a majority decision, the Committee may request the review of any subcommittee's decisions or activities.

Section 4.

Each subcommittee of the Committee shall meet as often as the subcommittee members find to be necessary.

Section 5.

All subcommittees shall be ad hoc in nature, and sit at the pleasure of the Committee Chair and a majority vote of the membership present at the time of the subcommittee creation.

ARTICLE VII: OFFICERS AND DUTIES

Section 1.

The officers of the Committee shall be the Chairperson (Chair) and the Vice Chairperson (Vice Chair).

Section 2.

The Chairperson shall be chosen by the Executive Director of the Office of Emergency Services from among members of the Committee, and shall serve at the pleasure of the Director. The Vice Chair shall be chosen by the membership of the Committee from among members of the Committee.

Section 3.

The Chair shall preside over all meetings of the Committee, and perform such additional duties as requested by the Committee and normally executed by a chairperson. The Chair shall create such standing and ad hoc committees as are deemed necessary to carry out the powers, duties and mission of the Committee. The Chair also shall appoint all members to both standing and ad hoc committees. All such subcommittee members shall serve at the pleasure of the Chair.

Section 4.

In the absence of the Chair, the Vice Chair shall preside at meetings and perform such additional duties as are required by the Committee and necessitated by the absence of the Chair.

Section 5.

In the event a vacancy occurs in the office of the Chairperson, the Director shall designate a successor prior to the next regular or special meeting. In the event a vacancy occurs in the office of the Vice Chairperson, the membership of the Committee shall designate a successor at the next regular or special meeting (Penal Code 13810).

ARTICLE VIII: QUORUM, VOTING AND ATTENDANCE

Section 1.

A quorum of the Committee for any meeting shall consist of a majority of the members designated or appointed at the time of the meeting. If a quorum is present, a majority vote of the members present is necessary for Committee action, except for the suspension of these bylaws pursuant to Article XII.

Section 2.

No vote by an alternate will be honored except as provided for in this section.

- a) An alternate designation letter is required from any absent Committee member, and shall be presented to the Committee prior to the start of the next regular or special meeting.
- b) An alternate will have full voting rights, floor rights, and be included in quorum determinations.
- c) Alternated attendance for a Committee member will negate provision of Section 3 below.

Section 3.

Any member of the Committee who misses three consecutive meetings or who attends less than fifty percent of the Committee's regularly called meetings during one calendar year shall be automatically removed from the Committee, except in situations in which the Chair finds that such deficiency is the result of illness or injury.

ARTICLE IX: REIMBURSEMENT OF EXPENSES

Section 1.

Members of the Committee shall not receive compensation for their services but will be reimbursed for those actual and necessary expenses incurred which relate to their duties as Committee members.

Section 2.

Members of continuing task forces, review committees or of any other Committee-established auxiliary bodies who are not Committee members shall not receive compensation for expenses, unless prior approval has been obtained from the Office of Emergency Services. However, individuals who appear before the Committee at its request in order to review specific topics on one or more occasions shall be reimbursed for their necessary travel expenses.

ARTICLE X: EXECUTIVE SECRETARY

Section 1.

The Executive Secretary of the Committee shall be appointed by the Director of the Office of Emergency Services

Section 2.

The duties of the Executive Secretary to the Committee shall be to provide staff support to the Committee including keeping all records, preparing agendas for each meeting, keeping minutes and approving all Committee expenditures.

Section 3.

The Executive Secretary shall, in accordance with applicable law, be responsible for any additional staffing, planning, organizing, coordinating, and directing to those activities necessary to assure the fulfillment of the powers, duties, and mission of the Committee.

ARTICLE XI: CONFLICT OF INTEREST

Section 1.

No member of the Committee shall participate personally through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise in any proceeding, application, request for a ruling or other determination, contract, grant claim controversy, or other particular matter in which funds under jurisdiction of the Committee are used, where to his or her knowledge he or she or his or her immediate family, partners, organization other than a public agency in which he or she is serving is an officer, director, trustee, partner, or employee or any person or organization with who he or she is negotiating or has any arrangement concerning prospective employment, has a financial interest.

Section 2.

In the review of proposals under appeal before the Committee, members of the Committee shall avoid any action which might result in, or create the appearance of:

- a) Using his or her official position for private gain
- b) Giving preferential treatment to any person
- c) Losing complete independence or impartiality
- d) Making an official decision outside official channels
- e) Affecting adversely the confidence of the public in the integrity of the Government or the program.

ARTICLE XII: AMENDMENTS TO THE BYLAWS

Section 1.

Amendments